属性ベース署名を用いた匿名シングルサインオンの提案 (言語、論理、代数系と計算機科学の展開)

AUTHOR(S):

堀川, 航洋; 高谷, 眞弓; Fazekas, Szilárd Zsolt; 山村, 明弘

CITATION:

堀川, 航洋 ...[et al]. 属性ベース署名を用いた匿名シングルサインオンの提案 (言語、論理、代数系と計算機科学の展開). 数理解析研究所講究録 2017, 2051: 158-166

ISSUE DATE:

2017-10

URL:

http://hdl.handle.net/2433/237105

数理解析研究所講究録
第2051巻 2017年 158-166

属性ベース署名を用いた匿名シングルサインオンの提案

堀川航洋，高谷眞弓，Szilárd Zolt Fazekas，山村明弘

秋田大学

1 はじめに

1.1 背景と目的

インターネットの普及に伴い，ユーザは普段から様々なサービスプロバイダにアクセスするようになった．ユーザは，複数のサービスプロバイダに対してそれぞれID/ パスワードのペアを用意するか，同じもしくは似たようなID/パスワードのペアを利用する，というどちらか方法をとる．これらの方法は非常に不便であるか，セキュリティの面で危険である．実際，ID/パスワードを使いまわしているユーザは9割にのぼることが報告されている．アカウントリスト攻撃はこのような使い回しに対する攻撃であり，一つのID/パスワードの流出により，多大な被害を及ぼす可能性がある．シングル・サインオン (SSO) はこれらの状況を回避する手法の一つである．SSO は1988 年に Steiner らによって提案された Kerberos[12] から始まり，他にも OpenID[13] など様々な SSO 方式が提案されてきた．しかし，多くの SSO 方式は欠点を有している．例えば Dodson らが提案した方式 [14] では，ユーザが証明書を利用してサービスプロバイダにアクセスする場合，サービスプロバイダは証明書の有効性を検証できないため信頼できる第三者機関と直接通信する必要がある．中里等がペアリングを用いて初めて SSO の匿名性を形式化した [19]。Wang らはそれに続き、匿名シングルサインオン（ASSO）を形式化した．Wang らの ASSO 方式 [10] は動的グループ署名 [1] を変換することにより実現されている．動的グループ署名，ユーザが何らかのグループに属するという証明を用いて署名する方式であり，この証明をサービスプロバイダにおける認証に利用している．しかしこの方式では，ユーザが特定のグループに所属しているか否かという点でしか認証を行うことができず，柔軟性に欠ける．本論文では Maji らによって提案された属性ベース署名（ABS）[7][8] を変換することで，属性を用いたより柔軟な認証を行うことができる ASSO 方式を提案することを目的とする．まず，2 章において Wang らの ASSO 方式について，要件とセキュリティの定義について述べる．3 章では ABS について説明し，4 章において ABS を利用した ASSO 方式について述べ，最後にまとめと今後の課題について触れる．

1.2 シングル・サインオン

ユーザはサービスプロバイダを利用する際，自身の持つID/パスワード等を提示し，ログインの手続きを行うことによりサービスを利用する．利用するサービスプロバイダが増えるにつれ，ユーザのID/パスワードの管理も難しくなる．複数のサービスプロバイダにおいて，ID/パスワードを使いまわすことはセキュリティ上の危険も大きく，アカウントリスト攻撃などの対象になりうる．そこで，ユーザの負担を減らし必要十分なセキュリティを保つためにSSOを導入する必要がある．SSOにおいてユーザは，一度だけ信頼できる第三者機関（TTP）を通して認証することで，複数のサービスプロバイダを利用することができる．これにより，ユーザはサービスプロバイダごとにID/パスワードのペアを入力する必要がなくなる．

1.3 匿名性

匿名とは，何らかの行動をとった人物が誰なのかを特定できない状態のことである．個人のプライバシーを保護することを目的とする．匿名性はレベルによってそれぞれ以下のように分類される．

- 非連結性

  任意の行動A，Bに対して，Aを行った人物とBを行った人物が同一であるかどうか判定できないことをUnlinkability(非連結性)と呼ぶ．例えば，各人にペンネームやハンドルネームといった偽名を割り振れば，匿名性は確保できるがUnlinlinkability は満たされない．

- 否認不可能性

  任意の行動Aを行ったのが自身でないことを第三者に対して証明できるときdeniable (否認可能) であるといい，そうでないときundeniable(否認不可能) であるという．

  匿名という言葉は2つにわけられ，Unlinkability を満たさなければ匿名といわない場合と，Unlinkability を満たさない場合でも匿名ということがある．これら2つを区別するために，Unlinkability を満たさない場合の匿名性をPsedonymity(偽名性) と呼ぶことがある．

2 Wang らの匿名シングルサインオン

INCoS-2013 においてWang らによって提案された匿名シングルサインオン (ASSO) について説明する．Wang らのASSO は動的グループ署名 (DGS) を変形することにより匿名でのSSOを実現している．

2.1 要件定義

ASSOの要件を以下のように定義する.

- ユーザは信頼できる第三者機関から一度，資格情報を取得すれば，資格情報から生成されるユーザ証明を利用して複数のサービスプロバイダにアクセスすることができる.
- サービスプロバイダは各ユーザが正当であるかどうかを検証することができるが，ユーザの身元を追跡することはできない.

2.2 構成

次に，ASSOの構成について説明する．ASSOはユーザ，信頼できる第三者機関(TTP)，サービスプロバイダ(SPs)により，以下の3つのアルゴリズムと1つのプロトコルが実行される.

- Setup :

  セキュリティパラメータ 1^k を入力として，(tpk, tik) のペアを出力する．ここで．tpk はTTPの公開鍵であり，tik はTTPの秘密鍵である.

- Enrol :

  ユーザはEnrol ProtocolをTTPとともに実行することによってシステムに登録することができる.

  1. ユーザ U_i は自身の公開鍵/秘密鍵のペア (upk_i, usk_i) を生成し，公開鍵 upk_i をTTPに送信する.
  2. TTPは登録規約に応じて U_i を受諾するか判断し tik を用いて U_i に対する登録情報 reg_i を生成する。
  3. reg_i を登録テーブル **reg** にコピーし，ユーザに送信する.
  4. U_i はTTPから受け取った reg_i と usk_i から生成される署名鍵 sk_i を資格情報 $Cre_i = (reg_i, sk_i)$ とする.

- UPGen :

  TTPの公開鍵 tpk，U_i の資格情報 $Cre_i = (reg_i, sk_i)$ とメッセージ m を入力とし，Cre_i の知識を示すユーザ証明を出力する.

- UPVer :

  TTPの公開鍵 tpk，メッセージ/ユーザ証明のペア (m, up_i) を入力として，有効なユーザ証明であれば1，そうでなければ0を出力する．サービスプロバイダは出力の値に応じてユーザのアクセスを受諾もしくは拒否する.

3 属性ベース署名を用いた匿名シングルサインオンの提案

属性ベース署名（ABS）を用いた匿名シングルサインオン（ASSO）について述べる．Wangらによって提案されたASSOは動的グループ署名を変形したものであったが，本研究においては動的グループ署名の代わりにABSを変形させることでASSOを実現する．

3.1 暗号的仮定と用いる概念

3.1.1 巡回群と双線型ペアリング

$\mathbb{G}, \mathbb{H}, \mathbb{G}_T$ を素数 p を位数とする巡回群とする．G を $\mathbb{G}$，H を $\mathbb{H}$ の生成元とする．$e(G,H)$ が $\mathbb{G}_T$ の生成元である場合，すべての a, b に対して $e:(G^a, H^b) = e(G,H)^{ab}$ である．このような巡回群に関する基本となる暗号的仮定を以下に示す．

- **q-SDH 仮定**

  q-Strong Diffie-Hellman仮定は，与えられた要素 $(G, G^x, ..., G^{x^q}, H, H^x) \in \mathbb{G}^{q+1} \times \mathbb{H}^2$，ランダムに選んだ $x \leftarrow \mathbb{Z}_p$，ランダムに選んだ生成元 $G \in \mathbb{G}, H \in \mathbb{H}$ に対して $(c, G^{\frac{1}{x+c}}) \in \mathbb{Z}_p \times \mathbb{G}$ となる任意のペアが計算上実行不可能であるとき，$(\mathbb{G}, \mathbb{H})$ において保たれる．

- **SXDH 仮定**

  External Diffie-Hellman 仮定は，標準的な決定的 Diffie-Hellman（DDH 仮定）が $\mathbb{G}, \mathbb{H}$ において同時に成り立つ場合，$(\mathbb{G}, \mathbb{H})$ において保たれる．

3.1.2 属性と認証規約

属性とは，各人に共通して備わっている性質や特徴のことである．ここでは性別，年齢，居住地や所属などが扱われる．属性はTTPがユーザの提示したライセンスなどに応じて発行する．提案方式においては，各ユーザはいくつかの属性に関連付けられている．このことにより，各ユーザは自身の身元を明かすことなく，匿名で認証を行うことを可能とする．はじめに，サービスプロバイダがユーザのアクセスを制御するための認証規約を定義する．認証規約は単調ブール関数であり，ブール関数をアクセスツリーとして表示する．ここで，内部ノードはANDとORゲートを，葉ノードはサービスプロバイダが要求する属性に対応する．例えば，A OR (B AND C) OR (D AND E) で表すことができる認証規約を考える．ここでA〜Eはそれぞれ属性を表す．この式においては属性 (B, D) もしくは (D, E) をもつ全てのユーザが認証規約を満たすことができる．次に，ブール関数を等価の行列へと変換する．ツリーのルートノードに長さ1のベクトル(1)をラベリングすることから始める．グローバル変数cを定義し，1に初期化する．親ノードがベクトル $\vec{a}$ によってラベル付けされたORゲートである場合，その子ノードにラベル付けをする．親ノードがベクトル $\vec{a}$ でラベル付けされたANDゲートである場合，左の子ノードはベクトル $a|1$ でラベル付けし，右の子ノードはベクトル $(0, ..., 0)| - 1$ でラベル付けする．ここで，$(0, ..., 0)$ は長さcのゼロベクトルを示す．最後にcの値を1だけインクリメントする．ツリー全体のラベル付が完了すると，葉ノードをラベル付けするベクトルは，LSSS行列

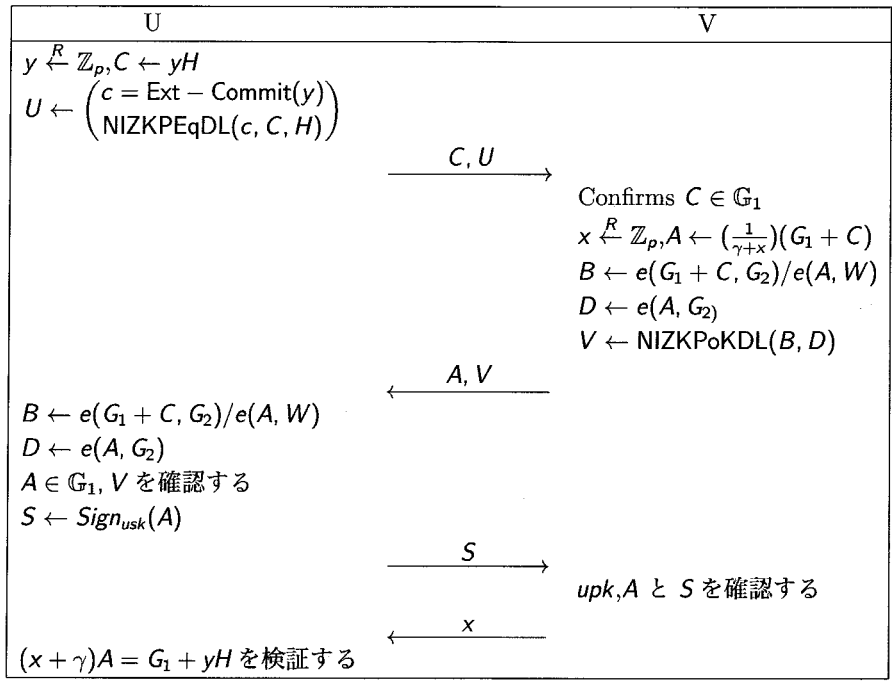

図 1: Join プロトコル

の行を形成する．これらのベクトルの長さが異なる場合は，末尾に 0 をつけることで同じ長さのベクトルになるように調節する．
上記の方法を用いることで，有限体 $\mathbb{F}$ 上の認証規約 Υ を単調スパンプログラム $\mathbf{M}$ に変換することができる．$\mathbf{M}$ は $\ell \times t$ の行列であり，ℓ は長さ， t は幅を示す．ここで，入力となる変数 $(x_1, ..., x_n) \in \{0,1\}^n$ を $\mathbf{M}$ の各行に関連付けるラベル付け関数 $a : [\ell] \to [n]$ を設定する．単調スパンプログラムは以下の基準で入力を受諾，もしくは拒否する．

$$\begin{aligned} \Upsilon(x_1, ..., x_n) &= 1 \Leftrightarrow \exists \vec{v} \in \mathbb{F}^{1\times\ell} \\ &\quad s.t.\, \vec{v}\mathbf{M} = [1, 0, ..., 0] \; and \; (\forall i : x_{a(i)} = 0 \Rightarrow v_i = 0) \end{aligned}$$

すなわち，$\{i \mid x_{a(i)=1}\}$ によりインデックスされた $\mathbf{M}$ の行の線形結合がベクトル $[1, 0, 0, ..., 0]$ を張る場合にのみ， $\Upsilon(x_1, ..., x_n) = 1$ となる．

3.1.3 Join プロトコル

偽造不可能を保証するためには，信頼できる第三者機関が秘密鍵を知らないような証明書をユーザに提供する特定の手順が必要となる． Join プロトコルにおいて，ユーザは信頼できる第三者機関と対話して，自身の秘密情報 y を含む有効な証明書 (A, x, y) を得る．ここで，

Ext − Commit は関数であり，トラップドアによって明らかにできる．トラップドアは偽造不可能性のセキュリティ証明のシミュレータを除いて誰にも知られることはない．
NIZKPEqDL(c, C, H) は非対話ランダムオラクルモデルであり，生成元 H における C の離散対数と計算された値 c の等価性の証明であるとともに知識の証明に用いられる．このとき，ユーザーは必ず C を知っている．
NIZKPoKDL(B, D) は非対話ランダムオラクルモデルであり，D における B の離散対数の知識のゼロ知識証明を示す．このプロトコルは，すべての証明が非対話 (NIZKPEqDL，NIZKPoKDL，および署名) であり，すべての証明が最初の 2 回のフローで定義されているので，このプロトコルは安全である．最後の 2 回のフローには，証明書がユーザーに公開される前に署名が含まれており，これは偽造不可能性を保証する．

3.2 ABS を用いた ASSO の構成

- ASSO.PSetup:

  1. 素数 p を位数とする巡回群 $\mathbb{F}, \mathbb{G}, \mathbb{H}$ を選択し，双線型ペアリング $e : \mathbb{G} \times \mathbb{H} \to \mathbb{G}_T$ を設定する．
  2. 衝突困難ハッシュ関数 $\mathcal{H} : \{0,1\} \to \mathbb{Z}_p^*$ を選択する．
  3. ランダムな生成元 $F \leftarrow \mathbb{F}$，$G_1, G_2 \leftarrow \mathbb{G}$，$H, H_0, ..., H_t \leftarrow \mathbb{H}$ を選択する．
  4. 乱数 $a_0, a, b, c \leftarrow \mathbb{Z}_p^*, \gamma \leftarrow \mathbb{Z}_p$ を選択する．
  5. $W = \gamma G_1$，$C = G^c$，$A_0 = H_0^{a_0}$，$A_j = H_j^a$，$B_j = H_j^b$ $[\forall j \in t]$ を設定する．
     秘密鍵 $ASK = (a_0, a, b, \gamma)$ とし，公開鍵 $APK = (A_0, ..., A_t, B_1, ..., B_t, C, W)$ および参照情報 $TPK = (\mathbb{F}, \mathbb{G}, \mathbb{H}, \mathcal{H}, G_1, G_2, H, H_0, ..., H_t)$ を公開する．

- ASSO.USetup :

  1. ユーザは乱数 $y \leftarrow \mathbb{Z}_p$ を選択し，$X \leftarrow yH$ を設定する．
  2. 信頼できる第三者機関との間で Join プロトコルを実行する．
  3. 登録証明 (A, x, y) を得る．

  − ASSO.AtrrGen :

  ユーザの属性集合 $\mathcal{A} \subseteq \mathbb{A}$ と秘密鍵 ASK を入力とする．

  1. ランダムに生成元 $K_{base} \leftarrow \mathbb{G}$ を選択する．
  2. $K_0 = K_{base}^{1/a_0}$，$K_u = K_{base}^{1/(a+bu)}$ $(\forall u \in \mathcal{A})$ を設定する．
  3. 署名鍵 $SK_{\mathcal{A}} = (K_{base}, K_0, \{K_u | u \in \mathcal{A}\})$ としてユーザに送信する．

- ASSO.Sign

公開鍵のペア $PK = (APK, TPK)$，署名鍵 $SK_{\mathcal{A}}$，メッセージ m，サービスプロバイダが要求する Υ を入力とする．

1. Υ を Υ のラベル付とともに，対応する単調スパンプログラム $\mathbf{M} \in (\mathbb{Z}_p)^{\ell \times t}$ に変換する．
2. 自身の属性 $\mathcal{A}$ に対応するベクトル $\vec{v}$ と $\mu = \mathcal{H}(m \| \Upsilon)$ を計算する．
3. 乱数 $r_0 \leftarrow \mathbb{Z}_p^*$ と $r_1, .., r_\ell \leftarrow \mathbb{Z}_p$ を選択し以下を計算する．

$$Y = K_{base}^{r_0},\ S_i = (K_{u(i)}^{v_i})^{r_0} \cdot (CG^{\mu})^{r_i}\ (\forall i \in [\ell])$$

$$Z = K_0^{r_0},\ P_j = \prod_{i=1}^{\ell} (A_j B_j^{u(i)})^{\mathbf{M}_{ij} \cdot r_i}\ (\forall j \in [t])$$

4. 登録証明から以下の検証式 T_1, T_2, T_3 を生成する．

$$T_1 = e(A, G_2)^x,\ T_2 = e(A, W),\ T_3 = e(H, G_2)^{-y}$$

5. 署名 $\sigma = (Y, W, S_1, ..., S_\ell, P_1, ..., P_t, T_1, T_2, T_3)$ とし，(m, σ) をサービスプロバイダに送信する．

- ASSO.Ver :

公開鍵のペア $PK = (APK, TPK)$，署名 σ，メッセージ m，認証規約 Υ を入力とする．

1. Υ を $u : [\ell] \to \mathbb{A}$ のラベル付とともに，対応する単調スパンプログラム $\mathbf{M} \in (\mathbb{Z}_p)^{\ell \times t}$ に変換する．
2. $\mu = \mathcal{H}(m || \Upsilon)$ を計算し，以下の式を検証する．

$$e(A, G_2)^x \cdot e(A, W) \cdot e(H, G_2)^{-y} = e(G_1, G_2)$$

$$e(Z, A_0) = e(Y, h_0)$$

$$\prod_{i=1}^{\ell} e(S_i, (A_j B_j^{u(i)})^{M_{ij}}) = \begin{cases} e(Y, h_1) e(Cg^{\mu}, P_1), & j = 1 \\ e(Cg^{\mu}, P_j), & j > 1 \end{cases}$$

すべての式を正しく確認した場合，アルゴリズム ASSO.Ver は accpet を出力する．

3. 最後に，サービスプロバイダはユーザのアクセスを許可する．

3.3 要件とセキュリティ定義

提案方式においても，WangらのASSOと同様の要件定義を用いる．セキュリティ定義については，以下のように設定する．

- 正当性：

  すべての $PK = (TPK, APK) \leftarrow$ ASSO.PSetup，メッセージ m，属性集合 $\mathcal{A}$，署名鍵 $SK_{\mathcal{A}} \leftarrow$ ASSO.AttrGen$(ASK, \mathcal{A})$，$\Upsilon(\mathcal{A}) = 1$ となるような認証規約 Υ，
  署名 $\sigma \leftarrow$ ASSO.Sign$(PK, SK_{\mathcal{A}}, m, \Upsilon, T_1, T_2, T_3)$ に対して，ASSO.Ver$(PK, m, \Upsilon, \sigma, T_1, T_2, T_3) = 1$ となるとき，提案方式は正当であるという．

- 匿名性：

  異なる属性の集合 $\mathcal{A}_1$，$\mathcal{A}_2$ から生成される署名 σ が等価であり識別できないとき，提案方式は匿名であるという．

- 偽造不可能性：

  以下の2つが満たされるとき，本方式は偽造不可能であるという．

  1. 敵対者が各々が持つ属性を集めることにより新たな署名を生成し認証できない．
  2. ユーザおよび信頼できる第三者機関は，サービスプロバイダの検証を通過する署名を単独で作成することができない．

4 まとめと課題

本論文では，ABSを用いたASSO方式を提案した．属性の概念を導入することにより，サービスプロバイダが必要とする属性を規約として認証に用いることが可能となった．グループに所属しているか否かという2値でしか認証することができないWangらの方式と比べて，提案方式は柔軟な認証を行うことができると考えられる．課題として，詳細なセキュリティ証明を行う，ユーザの属性の変更や失効を可能にする，といった点があげられる．セキュリティの証明に関して，今回は安全性の証明を行えていない．ゲームベース定義による提案方式全体の安全性を証明する必要がある．
ユーザの属性に関しては，変更や失効といった機能が必要である．実生活の変化に伴い，ユーザの属性が変わったり，増減するといったことが考えられる．それに対応できるよう機能を拡張する必要がある．

参考文献

[1] Bellare, Mihir *Foundations of Group Signatures : The Case of Dynamic Groups.* 2005

[2] Camenisch, Jan and Groß, Thomas *Efficient Attributes for Anonymous Credentials.* 2010

[3] Delerablée, Cécile and Pointcheval, David*Dynamic fully anonymous short group signatures.* Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 2006

[4] Hinek, M J and Jiang, S and Safavi, R and Shahandashti, S F *Attribute-Based Encryption with Key Cloning Protection.* Science And Technology, 2008

[5] Karchmer, M and Wigderson, A *On Span Programs.* 1993

[6] Khader, Dalia Daoud *Attribute Based Authentication Schemes submitted by University of Bath Attribute Based Authentication Schemes Dalia Daoud Khader.* 2009

[7] Maji, Hemanta K *Attribute-Based Signatures : Achieving Attribute-Privacy and Collusion-Resistance.* 2008

[8] Maji, Hemanta K *Attribute-Based Signatures.* 2010

[9] Wang, Jingquan *Transforming digital signatures into single sign-on schemes.* 2013

[10] Wang, Jingquan and Wang, Guilin and Susilo, Willy *Anonymous single sign-on schemes transformed from group signatures.* 2013

[11] Okamoto, Tatsuaki and Takashima, Katsuyuki *Efficient attribute-based signatures for non-monotone predicates in the standard model.* 2014

[12] Massachusetts Institute of Technology *Kerberos: The Network Authentication Protocol.* https://web.mit.edu/kerberos/, 1989

[13] OpenID Foundation *OpenID website.* http://openid.net/, 2005

[14] Dodson, Ben E N and Sengupta, Debangsu and Boneh, Dan a N and Lam, Monica S *Secure , Consumer-Friendly Web Authentication and Payments with a Phone.* 2010

[15] Ruj, Sushmita and Stojmenovic, Milos and Nayak, Amiya *Privacy Preserving Access Control with Authentication for Securing Data in Clouds.* 2012

[16] Wang, Cong and Member, Student and Chow, Sherman S M and Wang, Qian and Member, Student and Ren, Kui and Lou, Wenjing*Privacy-Preserving Public Auditing for Secure Cloud Storage.*

[17] Beimel, Amos and Beimel, Amos *Secure Schemes for Secret Sharing and Key Distribution for the degree of Doctor of Science.*

[18] Belenkiy, Mira and Chase, Melissa and Kohlweiss, Markulf and Lysyanskaya, Anna *P-signatures and Noninteractive Anonymous Credentials.* 2008

[19] J.Nakazato, L.Wang, A.Yamamura, Privacy enhancing credentials, ASIAN2007, Lecture Notes in Computer Science, Vol. 4846, 55–61, 2007